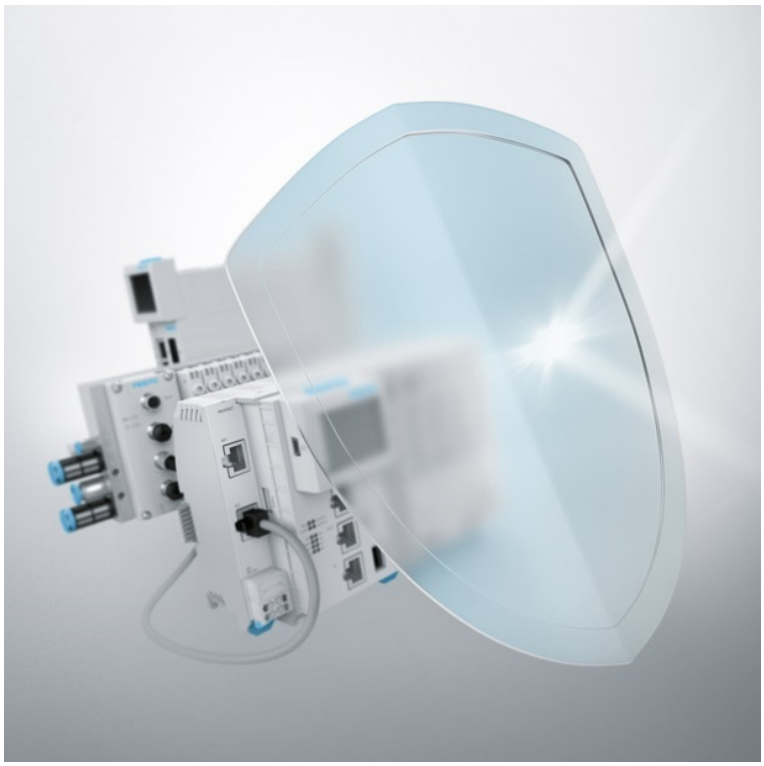
Incomplete documentation of remote accessible functions and protocols in Festo products



FSA-202209

Date
December 13th, 2022

Creator
Festo SE & Co. KG

Version
1.1.0

Festo SE & Co. KG

www.festo.com/psirt
psirt@festo.com
Ruiter Straße 82
73734 Esslingen
GERMANY

Summary

Incomplete Festo product documentation of remote accessible functions and their required IP ports. Depending on the product a description of the supported features can be found in the product documentation to some extent.

Festo developed the products according to the respective state of the art. As a result, the protocols used no longer fully meet today's security requirements. The products are designed and developed for use in sealed-off (industrial) networks. If the network is not adequately sealed off, unauthorized access to the product can cause damage or malfunctions, particularly Denial of Service (DoS) or loss of integrity.

Vulnerability Identifier

CVEs: CVE-2022-3270

Severity

9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected Vendors

FESTO

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
Operator unit CDPX: Operator unit CDPX all versions affected	Festo:Ordercode:CDPX-X-A-W-4, CDPX-X-A-W-7, CDPX-X-A-W-13, CDPX-X-A-S-10	For CVE-2022-3270 (Score: 9.4; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Controller CECC: Controller CECC all versions affected	Festo:Ordercode:CECC-D, CECC-D-BA, CECC-LK, CECC-S	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:H/I:H/ A:H): Update of technical user manual documentation in next product version.
Controller CECC-X: Controller CECC-X all versions affected	Festo:Ordercode:CECC-X-*	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:H/I:H/ A:H): Update of technical user manual documentation in next product version.
Controller CECX-X-C1: Controller CECX-X-C1 all versions affected	Festo:Partnumber:553852 Festo:Ordercode:CECX-X-C1	For CVE-2022-3270 (Score: 9.4; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:L/I:H/ A:H): Update of technical user manual documentation in next product version.
Controller CECX-X-M1: Controller CECX-X-M1 all versions affected	Festo:Partnumber:553853 Festo:Ordercode:CECX-X-M1	For CVE-2022-3270 (Score: 9.4; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:L/I:H/ A:H): Update of technical user manual documentation in next product version.
Camera system CHB-C-N: Camera system CHB-C-N all versions affected	Festo:Partnumber:3501040 Festo:Ordercode:CHB-C-N	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:H/I:H/ A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Motor controller CMMO-ST: Motor controller CMMO-ST all versions affected	Festo:Ordercode:CMMO-ST-C5-1-DIOP, CMMO-ST-C5-1-DION, CMMO-ST-C5-1-LKP	For CVE-2022-3270 (Score: 7.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.
Motor controller CMMP-AS: Motor controller CMMP-AS all versions affected	Festo:Ordercode:CMMP-AS-*	For CVE-2022-3270 (Score: 8.2; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.
Motor controller CMMT-AS: Motor controller CMMT-AS all versions affected	Festo:Ordercode:CMMT-AS-*	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Controller CMXH: Controller CMXH all versions affected	Festo:Partnumber:3605478 Festo:Ordercode:CMXH-ST2-C5-7-DIOP	For CVE-2022-3270 (Score: 7.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.
Control block CPX-CEC: Control block CPX-CEC all versions affected	Festo:Ordercode:CPX-CEC, CPX-CEC-C1, CPX-CEC-M1, CPX-CEC-C1-V3, CPX-CEC-S1-V3, CPX-CEC-M1-V3	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Control block CPX-CMXX: Control block CPX-CMXX all versions affected	Festo:Partnumber:555667, 555668 Festo:Ordercode:CPX-CMXX	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.
Controller CPX-E-CEC: Controller CPX-E-CEC all versions affected	Festo:Ordercode:CPX-E-CEC-*	For CVE-2022-3270 (Score: 9.4; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB32: Bus node CPX-FB32 all versions affected	Festo:Partnumber:541302 Festo:Ordercode:CPX-FB32	For CVE-2022-3270 (Score: 7.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB33: Bus node CPX-FB33 all versions affected	Festo:Partnumber:548755 Festo:Ordercode:CPX-FB33	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-M-FB34: Bus node CPX-M-FB34 all versions affected	Festo:Partnumber:548751 Festo:Ordercode:CPX-M-FB34	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Bus node CPX-M-FB35: Bus node CPX-M-FB35 all versions affected	Festo:Partnumber:548749 Festo:Ordercode:CPX-M-FB35	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB36: Bus node CPX-FB36 all versions affected	Festo:Partnumber:1912451 Festo:Ordercode:CPX-FB36	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB37: Bus node CPX-FB37 all versions affected	Festo:Partnumber:2735960 Festo:Ordercode:CPX-FB37	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB39: Bus node CPX-FB39 all versions affected	Festo:Partnumber:2093101 Festo:Ordercode:CPX-FB39	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB40: Bus node CPX-FB40 all versions affected	Festo:Partnumber:2474896 Festo:Ordercode:CPX-FB40	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Control block CPX-FEC-1-IE: Control block CPX-FEC-1-IE all versions affected	Festo:Partnumber:529041 Festo:Ordercode:CPX-FEC-1-IE	For CVE-2022-3270 (Score: 8.2; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.
Gateway CPX-IOT: Gateway CPX-IOT all versions affected	Festo:Partnumber:8069773 Festo:Ordercode:CPX-IOT	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CTEU-EP: Bus node CTEU-EP all versions affected	Festo:Partnumber:2798071 Festo:Ordercode:CTEU-EP	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus node CTEU-PN: Bus node CTEU-PN all versions affected	Festo:Partnumber:2201471, 8107589 Festo:Ordercode:CTEU-PN, CTEU-PN-EX1C	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Integrated drive EMCA: Integrated drive EMCA all versions affected	Festo:Ordercode:EMCA-EC-67-*	For CVE-2022-3270 (Score: 7.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Planar surface gantry EXCM: Planar surface gantry EXCM all versions affected	Festo:Ordercode:EXCM-*	For CVE-2022-3270 (Score: 7.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H): Update of technical user manual documentation in next product version.
VTEM: VTEM all versions affected	Festo:Partnumber:8047502 Festo:Ordercode:VTEM-S1-*	For CVE-2022-3270 (Score: 9.4; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H): Update of technical user manual documentation in next product version.
Compact Vision System SBO..-Q: Compact Vision System SBO..-Q all versions affected	Festo:Ordercode:SBO*-Q-*	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.
Compact Vision System SBO..-C: Compact Vision System SBO..-C all versions affected	Festo:Ordercode:SBO*-C-*	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.
Compact Vision System SBO..-M: Compact Vision System SBO..-M all versions affected	Festo:Ordercode:SBO*-M-*	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Controller SBRD-Q: Controller SBRD-Q all versions affected	Festo:Partnumber:8067301 Festo:Ordercode:SBRD-Q	For CVE-2022-3270 (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:H/I:H/ A:H): Update of technical user manual documentation in next product version.
Bus node CPX-FB43: Bus node CPX-FB43 all versions affected	Festo:Partnumber:8110369 Festo:Ordercode:CPX-FB43	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/ AC:L/PR:N/UI:N/S:U/C:N/I:H/ A:H): Update of technical user manual documentation in next product version.
Bus node CPX-M-FB44: Bus node CPX-M-FB44 all versions affected	Festo:Partnumber:8110370 Festo:Ordercode:CPX-M-FB44	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/ AC:L/PR:N/UI:N/S:U/C:N/I:H/ A:H): Update of technical user manual documentation in next product version.
Bus node CPX-M-FB45: Bus node CPX-M-FB45 all versions affected	Festo:Partnumber:8110371 Festo:Ordercode:CPX-M-FB45	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/ AC:L/PR:N/UI:N/S:U/C:N/I:H/ A:H): Update of technical user manual documentation in next product version.
Servo drive CMMT-ST-C8-1C-EP-S0: Servo drive CMMT-ST-C8-1C-EP-S0 all versions affected	Festo:Partnumber:8084006 Festo:Ordercode:CMMT-ST-C8-1C-EP-S0	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/ AC:L/PR:N/UI:N/S:U/C:N/I:H/ A:H): Update of technical user manual documentation in next product version.

Affected Product and Versions	Product Details	Remediation
Servo drive CMMT-ST-C8-1C-PN-S0: Servo drive CMMT-ST-C8-1C-PN-S0 all versions affected	Festo:Partnumber:8084004 Festo:Ordercode:CMMT-ST-C8-1C-PN-S0	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus module CPX-E-EP: Bus module CPX-E-EP all versions affected	Festo:Partnumber:4080499 Festo:Ordercode:CPX-E-EP	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
Bus module CPX-E-PN: Bus module CPX-E-PN all versions affected	Festo:Partnumber:4080497 Festo:Ordercode:CPX-E-PN	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
EtherNet/IP interface CPX-AP-I-EP-M12: EtherNet/IP interface CPX-AP-I-EP-M12 all versions affected	Festo:Partnumber:8086610 Festo:Ordercode:CPX-AP-I-EP-M12	For CVE-2022-3270 (Score: 9.1; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.
EtherNet/IP interface CPX-AP-I-PN-M12: EtherNet/IP interface CPX-AP-I-PN-M12 all versions affected	Festo:Partnumber:8086607 Festo:Ordercode:CPX-AP-I-PN-M12	For CVE-2022-3270 (Score: 8.1; Vectorstring: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H): Update of technical user manual documentation in next product version.

Workarounds and Mitigations

Remediations can be found in the table of Affected Products and Recommendations.

Additionally, please refer to the General Recommendations.

Impact and Classification of Vulnerabilities

CVE-2022-3270
In multiple products by Festo a remote unauthenticated attacker could use functions of undocumented protocols which could lead to a complete loss of confidentiality, integrity and availability.
Weakness: Incomplete Documentation (CWE-1059)
Base Score: 9.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

General recommendations

Users running communication over an untrusted network who require full protection should switch to an alternative solution such as running the communication over a VPN.

Festo strongly recommends to minimize and protect network access to connected devices with state of the art techniques and processes.
For a secure operation follow the recommendations in the product manuals and note the protocols and their supported features in Festo Field Device Tool or Festo Automation Suite online help.

As part of a security strategy, Festo recommends the following general defense measures to reduce the risk of exploits:
- Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
- Use firewalls to protect and separate the control system network from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Use encrypted communication links
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control system by using up to date virus detecting solutions

Acknowledgments

Festo SE & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination and support with this publication (see: https://cert.vde.com/)
- Daniel dos Santos, Rob Hulsebos from Forescout for reporting to Festo (see: https://forescout.com/)

Publisher Details

https://festo.com/psirt

Festo SE & Co. KG, PSIRT, Ruiter Straße 82, 73734 Esslingen Germany, psirt@festo.com

For further security-related issues in Festo products please contact the Festo Product Security Incident Response Team (PSIRT) https://festo.com/psirt

Also refer to:

- https://cert.vde.com/en/advisories/VDE-2022-041
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/
- CVE entry at Mitre https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3270

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	November 29th, 2022	intial version
1.1.0	December 05th, 2022	added bus module CPX-E-PN as affected product

Sharing rules

TLP: WHITE
For the TLP version see: https://www.first.org/tlp

Disclaimer

Festo assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided free of charge and on good faith by Festo. Insofar as permissible by law, however, none of this

information shall establish any warranty, guarantee, commitment or liability on the part of Festo. Note: In no case does these information release the operator or responsible person from the obligation to check the effect on his system or installation before using the information and, in the event of negative consequences, not to use the information.

In addition, the actual general terms and conditions of Festo for delivery, payment and software use shall apply, available under http://www.festo.com.